ACTION
OCA 87-4049

OFFICE OF CONGRESSIONAL AFFAIRS

Routing Slip

	ACTION	INFO
1. D/OCA		X
2. DD/Legislation	XXX	
3. DD/Senate Affairs		X
4. Ch/Senate Affairs		
5. DD/House Affairs		X
6. Ch/House Affairs		
7. Admin Officer		
8. Executive Officer		
9. FOIA Officer		
10. Constituent Inquiries Officer		
11.		X
12.		

SUSPENSE 23 Sept 87
Date

STAT

Action Officer:

STAT

Remarks:

22 Sept 87
Name/Date

STAT

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503
September 17, 1987

O/CONGRESSIONAL AFFAIRS
87-4049

LEGISLATIVE REFERRAL MEMORANDUM

OCA FILE LEG

TO: **Legislative Liaison Officer**

SEE ATTACHED DISTRIBUTION LIST

SUBJECT: Department of Justice report on HR 145 - Computer Security Act.

The Office of Management and Budget requests the views of your agency on the above subject before advising on its relationship to the program of the President, in accordance with OMB Circular A-19.

A response to this request for your views is needed no later than

WEDNESDAY -- SEPTEMBER 23, 1987

Questions should be referred to Constance J. Bowers (395-3457), the legislative analyst in this office.

Gregory M. Jones Jr.

Assistant Director for Legislative Reference

Enclosures
cc: Ed Springer
Arnold Donahue
Kevin Scheid
Bob Damus
Bob Bedell

DISTRIBUTION LIST

AGENCY	CONTACT	PHONE NUMBER
Department of Defense (06)	Sam Brick	697-1305
Department of Energy (09)	Bob Rabben	586-6718
Department of Health and Human Services (14)	Frances White	245-7750
Department of Justice (17)	Jack Perkins	633-2113
Department of State (25)	Lee Howdershell	647-4463
Department of the Treasury (28)	Carole Toth	566-8523
Office of Personnel Management (22)	James Woodruff	632-5524
General Services Administration (37)	Al Vicchiolla	566-0563
National Security Council		
Central Intelligence Agency ✓		

U.S. Department of Justice

Office of Legislative and Intergovernmental Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

Honorable Gordon J. Humphrey
Subcommittee on Technology
and the Law
Committee on the Judiciary
United States Senate
Washington, D.C. 20510-6275

Dear Senator Humphrey:

This letter responds to your request for the views of the Department of Justice on Section 8 of H.R. 145, the Computer Security Act of 1987. For the reasons set forth below, the Department of Justice believes that this legislation might inadvertently have an adverse and unintended impact upon the implementation of the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552. While our concerns would be assuaged somewhat by the inclusion of language in the legislative history setting forth more clearly the intended construction of the bill, we believe that technical, clarifying amendments might be appropriate for consideration. We are hopeful that these concerns can be addressed before final action is taken on this bill.

This bill would establish a comprehensive scheme for the development of computer security plans for Federal computer systems which contain sensitive, but unclassified, information. Sensitive information is generally defined in the Act as information the loss, misuse, or unauthorized access to, or modification of which could adversely affect the national interest or the conduct of Federal programs or privacy to which individuals are entitled under the Privacy Act of 1974, 5 U.S.C. § 552a.

The protection of sensitive information as defined in H.R. 145 is of particular concern to the Department because of its law enforcement responsibilities. An unauthorized intrusion into the Federal Bureau of Investigation's or the Drug Enforcement Administration's computers could have extremely serious consequences. The Department has also become aware of an increasing number of FOIA requests for computer software pertaining to agency computer systems which contain "sensitive information" as defined in H.R. 145.

Provisions of the bill

Under Section 6 of the bill, agencies would be required to identify computer systems which contain sensitive data and to develop computer security plans for the privacy and security of these systems. These security plans undoubtedly would identify certain types of information pertaining to computer systems the release of which could reasonably be expected to pose a serious threat to the security of those systems, and therefore to the data contained in those systems. Such types of information could include physical security measures, personnel security measures, software security measures, equipment technical specifications, equipment location, encryption techniques for transmitting sensitive data, and operating software.

Section 8(1) of the bill provides that it shall not be construed to "constitute authority to withhold information sought pursuant to [the FOIA]." Section 8(2) of the bill further provides that it shall not be construed

> to authorize any Federal agency to limit, restrict, regulate, or control the collection, maintenance, disclosure, use, transfer, or sale of any information (regardless of the medium in which the information may be maintained) that is --
>
> (A) privately-owned information;
>
> (B) disclosable under [the FOIA], or other law requiring or authorizing the public disclosure of information; or
>
> (C) public domain information.

We understand that this language was included in the bill because, absent such a provision, it might have been possible to construe this Act as providing a new basis for withholding under the FOIA any information defined as sensitive information under it. Indeed, the legislative history generated in the House clearly indicates the sponsors' intention that the Act be "FOIA neutral," and that it not alter existing law with regard to disclosure of such information under the FOIA. 1/

Analysis of the Bill

1. Our principal concern with H.R. 145 relates to the disclosability of agency measures intended to ensure the security of its computer systems. While section 6 of the bill would

---

1/ See Computer Security Act of 1987, H.R. Rep. No. 153, 100th Cong., 1st Sess., pt. 1, at 31; pt. 2, at 30 (1987) ("House Report").

require agencies to establish plans for the security of these systems, the bill does not specifically authorize agencies to withhold such security plans (or other information relating to the implementation or effectiveness of computer security measures which they have determined should be restricted) from public disclosure, nor does any other statute specifically provide this protection.

Obviously, public disclosure of the various means adopted by agencies to ensure the security of their computer systems would compromise those security measures and substantially increase the risk that those systems (and the sensitive information they contain) could be improperly accessed and misused. We believe that, under present law, this information should be held to be properly protectible under Exemption 2 of the FOIA as well as Exemption 7 as amended, 5 U.S.C. § 552(b)(2), (b)(7), but the availability of such protection has yet to be considered by the courts. 2/

We are concerned, however, that Section 8(1) of the bill, as presently phrased, could be used by FOIA requesters to argue against the withholding of information pertaining to the security of Federal computer systems under existing law. Specifically, we fear that a requester seeking access to information pertaining to an agency's computer system (or to the agency's computer security plan itself) might argue that, had Congress intended such information to be withheld under the FOIA, it would have provided such protection in its comprehensive statutory scheme on this issue or, at the very least, would not have expressly disclaimed such protection without reservation. This is particularly so because the bill affirmatively requires the creation of crucial agency information -- the computer security plan itself -- yet provides no express protection for such plans. In short, we are concerned that, in context, the language of Section 8(1) might be argued not to be completely neutral.

This possible argument based on Section 8(1), should it ever succeed, would be extremely adverse to the government's and the public's interests and would be quite at odds with the stated purposes of this proposed Act, as well as the Computer Fraud and

---

2/ Neither the "agency record" status nor the nondisclosure of computer software per se has yet been considered by the courts, though some computer software reflecting auditing or investigative techniques has been found to be properly withheld under Exemptions 2 and 7(E) of the FOIA. See Windels, Marx, Davies & Ives v. Department of Commerce, 576 F. Supp. 405, 411-414 (D.D.C. 1983). See also Fiumara v. Higgins, 572 F. Supp. 1093, 1102 (D.N.H. 1983) (access codes and identification numbers of Treasury Enforcement Protection System held protectible under Exemption 2).

Abuse Act. 3/ Clearly the security of the computer systems themselves is a key element in safeguarding the information contained in agency computer systems, which is the primary focus of H.R. 145. 4/

To avoid even the possibility that Section 8(1) could be argued to prejudice the protection of computer security measures under existing law, the Department recommends that, at a minimum, the legislative history should reflect more clearly the express intention that any FOIA protection available under existing law (e.g., under Exemptions 2 and 7) would continue to be available for information pertaining to the security of federal computer systems containing sensitive information. If possible, we suggest that the language of Section 8(1) be modified slightly to provide that the Act shall not be construed "to constitute **any new** authority to withhold information sought pursuant to section 552 of title 5, United States Code." 5/

2. With respect to section 8(2) of this bill, we do not believe that this section was intended to create any new law with respect to the disclosure of electronically-stored data or software. As noted above, the legislative history generated in the House seems clear in its intention that this section apply only to information that has already been released under the FOIA or is privately owned or in the public domain.

However, we do recommend a technical amendment of the language of that section in order to avoid a possible interpretation that would be contrary to the stated intention. We recommend that the language of Section 8(2)(B) be modified to read: "(B) **required to be disclosed** under Section 552 of

---

3/ The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, 18 U.S.C. § 1030, as amended by the Computer Fraud and Abuse Act of 1986, reflects congressional concern with problems of computer security and unauthorized access by providing substantial fines and imprisonment for offenses related to unauthorized entry into federal computer systems.

4/ See House Report, pt. 1, at 23 ("The primary objective of this Act is controlling unauthorized use of the information in Federal computer systems, rather than merely protecting the computer systems themselves. Although computer hardware and software have real value and certainly must be safeguarded, it is the data . . . that represent the greatest vulnerability.") (emphasis added).

5/ Although those changes would at least help to avoid any negative implications from Section 8(1), it may also be appropriate to consider whether the bill should be amended to provide affirmative FOIA protection for the computer security information in question, should the opportunity to do so arise.

Title 5, United States Code . . . ." This change is suggested because all of the exemptions from disclosure in the FOIA are permissive rather than mandatory. All agency information, unless its disclosure is affirmatively prohibited by another law, can be released under the FOIA as a matter of administrative discretion, even if it is exempt from mandatory disclosure, and hence could be regarded as "disclosable" as a matter of FOIA routine. This suggested modification therefore is necessary to conform the language of this proposed section to the language of the FOIA and to the practicalities of FOIA practice.

Conclusion

For the foregoing reasons, the Department of Justice recommends consideration of technical amendments in order to avoid the possibility that this legislation might inadvertently have an adverse and unintended impact upon the implementation of the FOIA.

The Office of Management and Budget has advised this Department that there is no objection to the submission of this report from the standpoint of the Administration's program.

Sincerely,

John R. Bolton
Assistant Attorney General